Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) An information-processing apparatus serving as a data-processing means for carrying out predetermined processing OP1 on input data D1 in order to produce a result of said predetermined processing as processed data D2, said information-processing apparatus comprising:

a memory holding a table of candidates of disturbance data XI which maintains a constant Hamming weight before and after processing said disturbance data XI with said predetermined processing OP1;

a selector for selecting said disturbance data XI from said table;

a disturbance data processing means for ~~processing~~ performing said predetermined processing OP1 by using said disturbance data XI selected by said selector ~~with said predetermined processing OP1~~ in order to generate a disturbance data XO,

a data transform means for transforming said input data D1 by using said disturbance data XI ~~having a constant Hamming weight~~ selected by said selector, to generate transformed data H1~~, wherein said input data D1 does not have a constant Hamming weight~~;

a transformed-data-processing means for ~~carrying out~~ performing said predetermined processing OP1 ~~for~~ on said input data D1, or a processing different from said predetermined processing OP1 ~~to replace said predetermined processing~~

~~OP1~~ on said transformed data H1, in order to generate processed transformed data H2; and

a data inverse-transform means for ~~carrying out~~ performing an inverse-transformation processing OP2 on said processed transformed data H2 by using processed disturbance data XO ~~having a constant Hamming weight~~ generated by said disturbance-data-processing means, in order to generate said processed data D2 which can also be obtained without transformations as a result of said predetermined processing OP1 carried out on said input data D1.

2. (canceled)

3. (previously presented) An information-processing apparatus according to claim 1, wherein each bit of said processed disturbance data XO and said disturbance data XI has a logic value of 0 or 1 at a probability of 50%.

4. – 27. (canceled)

28. (new) An information-processing apparatus serving as a data-processing means for carrying out predetermined processing OP1 on input data D1 in order to produce a result of said predetermined processing as processed data D2, said information-processing apparatus comprising:

a memory holding a table of candidate pairs of disturbance data XI and disturbance data XO, wherein said disturbance data XI maintains a constant Hamming weight before and after processing said disturbance data XI with said

predetermined processing OP1, and wherein said disturbance data XO is obtained from said processing said disturbance data XI with said predetermined processing OP1,

a selector for selecting a pair of disturbance data XI and XO from said table,

a data transform means for transforming said input data D1 by using said disturbance data XI of a pair of said disturbance data XI and XO selected by said selector, to generate transformed data H1;

a transformed-data-processing means for performing said predetermined processing OP1 on said input data D1, or a processing different from said predetermined processing OP1 on said transformed data H1, in order to generate processed transformed data H2; and

a data inverse-transform means for performing an inverse-transformation processing OP2 on said processed transformed data H2 by using said disturbance data XO of said selected pair, in order to generate said processed data D2 which can also be obtained without transformations as a result of said predetermined processing OP1 carried out on said input data D1.